IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Newport News Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. 4:16cr16
	)	
EDWARD JOSEPH MATISH III,	)	
	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S FIRST MOTION TO SUPPRESS

Now comes the United States of America, by and through attorneys, Dana J. Boente, United States Attorney for the Eastern District of Virginia, and Kaitlin C. Gratton, Assistant United States Attorney, and submits its response to the defendant, EDWARD JOSEPH MATISH III's First Motion to Suppress information identifying his home computer recovered pursuant to a search warrant that authorized the use of a network investigative technique to recover such information. For the reasons set forth below, the defendant's motion should be denied.

INTRODUCTION

After a months-long investigation, the FBI briefly assumed administrative control of Playpen, a website dedicated to the sharing of child pornography. The FBI also sought and obtained a warrant permitting it to deploy a "Network Investigative Technique" (the "NIT") during that same period, which would cause a computer logging into Playpen to reveal certain identifying information—most importantly, its concealed Internet Protocol ("IP") address. Among the IP addresses identified accessing Playpen was one associated with Edward Matish III. Following the execution of a search warrant at Matish's home in Newport News, Virginia,

Matish was indicted and arrested on charges of accessing with intent to view child pornography involving a prepubescent minor. Matish now seeks to suppress the information obtained by the NIT and used to identify his home computer and its location, along with all other evidence derived from that information. For the reasons that follow, his motion should be denied.

First, the affidavit supporting the NIT warrant application established the need for the NIT to identify Playpen users and set forth ample probable cause to conclude that any users of Playpen knew of its illicit content and intended to access that content. As the affidavit explained, Playpen was no ordinary website, but a hidden service operating on an anonymous network that was dedicated to the sharing of child pornography. The magistrate judge who authorized the NIT warrant reasonably concluded that there was a fair probability that anyone who logged into Playpen did so with knowledge of its content and intent to view that content.

Second, the defendant makes no showing—much less a substantial, preliminary one—to justify a *Franks* hearing. He points to a change to the Playpen logo that occurred hours before the NIT warrant was authorized that was not included in the affidavit. But he does not offer any proof that this omission was intentional or reckless, nor can he. It was, at most, an innocent oversight. As important, the change—the replacement of two sexually suggestive photos of a prepubescent girl with a single sexually suggestive photo of a prepubescent girl—was immaterial. So, even if the defendant could somehow show the affiant acted intentionally or recklessly, he would not be entitled to relief. His remaining *Franks* arguments consist of little more than a disagreement with the opinions and conclusions of the veteran FBI agent contained within his affidavit, none of which suffice to justify a *Franks* hearing.

Third, the NIT warrant described the places to be searched and the items to be seized with particularity and was supported by probable cause. The Fourth Amendment demands

nothing more. The Court should not embrace the defendant's novel and unsupported constitutional rule—cloaked as a challenge to the warrant's particularity and overbreadth—that would find an otherwise valid warrant defective simply because it would authorize the search of a potentially large number of locations.

Fourth, the defendant's remaining criticisms of the NIT warrant are similarly unavailing and do nothing to aid his cause. Specifically, his claim that the NIT warrant was void because, as an anticipatory warrant, the "triggering event" never occurred is little more than a rehash of the same probable cause and *Franks* challenges he raises.

Finally, even if the NIT warrant were somehow flawed, the good faith exception is an independent bar to suppression. The NIT warrant affidavit set forth probable cause for its request to search particular locations for particular information. And a neutral and detached magistrate relied on that affidavit in authorizing the warrant. Law enforcement's reliance on that authorization was therefore objectively reasonable and suppression is thus unwarranted.

For these and the other reasons outlined below, the defendant's first motion to suppress should be denied.[1]

---

[1] The Government notes that the same arguments the defendant raises in support of his First Motion to Suppress have been raised and rejected in related litigations against other Playpen users. For example, on January 28, 2016, a district judge in the Western District of Washington rejected a defendant's argument that the same NIT warrant was an unconstitutional "general warrant." *United States v. Michaud*, No. 3:15-cr05351-RJB, 2016 WL 337263, *4-5 (W.D. Wa. Jan. 28, 2016). The judge had already orally denied the defendant's motion for a *Franks* hearing and his arguments that the NIT warrant lacked probable cause at the motions hearing. *Id.* at *1 & n.1. In *Michaud*, the Court ultimately concluded that "[t]he NIT warrant was supported by probable cause and particularly described the places to be searched and the things to be seized" and further concluded that the NIT warrant was executed in good faith. *Id.* at *8. The arguments presented in support of the motion to suppress in *Michaud* have since been raised in a related litigation, which was recently transferred to the same district judge. *See, e.g.*, Gov't Resp. to Def.'s Mot. to Supp. Evidence, Mar. 7, 2016, *United States v. Lorente*, No. 2:15cr-00274-RJB (W.D. Wa.) (ECF 48). Additionally, on March 14, 2015, a district judge in the Eastern District of Wisconsin adopted a sealed magistrate judge's report and recommendation denying a defendant's motion to suppress the NIT warrant. *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269, *1-2 (E.D. Wis. Mar. 14, 2016). In that case, the defendant argued that the NIT warrant "failed to establish probable cause, was not specific in describing how the NIT would find users of the web site and how it would make sure to find only users who engaged in illegal activity, and did not demonstrate that the NIT was likely to reveal evidence of a crime, and was unlimited in geographic scope." *Id.* at *1.

BACKGROUND

The charges in this case arise from an investigation into Playpen, a global online forum through which registered users (including the defendant) advertised, distributed, and/or accessed illegal child pornography. The scale of child sexual exploitation on the site was massive: more than 150,000 total members created and viewed tens of thousands of postings related to child pornography. Images and videos shared through the site were highly categorized according to victim age and gender, as well as the type of sexual activity. The site also included forums for discussion of all things related to child sexual exploitation, including tips for grooming victims and avoiding detection.

I. Playpen users, including Matish, used the Tor network to access child pornography while avoiding law enforcement detection

Playpen operated on the anonymous Tor network. Tor was created by the U.S. Naval Research Laboratory as a means of protecting government communications. It is now available to the public. The Tor network—and the anonymity it provides—is a powerful tool for those who wish to share ideas and information, particularly those living in places where freedom of speech is not accorded the legal protection it is here. But this anonymity has a downside. The Tor network is a haven for criminal activity in general, and the online sexual exploitation of children in particular. *See Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED MAGAZINE, December 30, 2014, available at: http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited March 31, 2016).

Use of the Tor network masks the user's actual IP address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called

"nodes) run by volunteers.[2] To access the Tor network, users must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle." Users can also access Tor through "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor. When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address. Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional IP-address-based identification techniques used by law enforcement on the open Internet are not viable.

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses. They operate the same as other public websites with one critical exception: namely, the IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client and operating in the Tor network. And unlike an open Internet website, it is not possible to use public lookups to determine the IP address of a computer hosting a "hidden service."

A "hidden service," like Playpen, is also more difficult for users to find. Even after connecting to the Tor network, users must know the exact web address of a "hidden service" in order to access it. Accordingly, in order to find Playpen, a user had to first get the web address for it from another source—such as another Playpen user or online postings identifying Playpen's content and location. Accessing Playpen thus required numerous affirmative steps by the user,

[2] Additional information about Tor and how it works can be found at www.torproject.org.

making it extremely unlikely that any user could have simply stumbled upon it without first understanding its child pornography-related content and purpose.

Although the FBI was able to view and document the substantial illicit activity occurring on Playpen, investigators faced a tremendous challenge when it came to identifying Playpen users. Because Tor conceals IP addresses, normal law enforcement tools for identifying Internet users would not work. So even if law enforcement managed to locate playpen and its IP logs, traditional methods of identifying users would have gone nowhere.

Acting on a tip from a foreign law enforcement agency, as well as information from its own ongoing investigation, the FBI determined that the computer server that hosted Playpen was located at a web-hosting facility in North Carolina. In February 2015, FBI agents apprehended the administrator of Playpen and seized the website from its web-hosting facility. Rather than immediately shut the site down, which would have allowed the users of Playpen to go unidentified (and un-apprehended), the FBI allowed it to continue to operate at a government facility in the Eastern District of Virginia for the brief period from February 20, 2015 through March 4, 2015.

In addition, the FBI obtained court authorizations from the United States District Court for the Eastern District of Virginia to (1) monitor the site users' communications, and (2) deploy a Network Investigative Technique ("NIT") on the site, in order to attempt to identify registered users who were anonymously engaging in the sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.[3]

Using the NIT, the FBI identified an IP address associated with Playpen user "Broden" and traced it to Edward Matish III. One July 23, 2015, FBI Task Force Agent Heather Call obtained a

[3] Publicly filed, redacted copies of the NIT search warrant, application, affidavit and return (No. 15-SW-89) are attached as Exhibit 1.

residential search warrant for Matish's home from The Honorable United States Magistrate Judge Tommy E. Miller. Agents executed the warrant at Matish's home on July 29, 2015. Matish was present at the home, was advised of the identities of the agents and the purpose of the search. He was further advised that he was free to leave while the search was being conducted and that he did not have to speak with agents. After receiving these advisements, Matish agreed to be interviewed. Among other things, Matish stated that he was familiar with the Tor network and acknowledged downloading the Tor browser. Matish denied ever creating an account on any Tor site or using the Tor network to view child pornography. Matish ultimately acknowledged accessing the Playpen site, but maintained that he had never logged into it.

On August 14, 2015, Matish voluntary appeared at the FBI for a pre-scheduled polygraph examination. After being advised of his constitutional rights and signing a form in which consented to an interview with polygraph, Matish underwent the examination. Following the test, Matish requested to type a statement in which he stated, among other things, that he had accessed and posted to the Playpen website. Matish also signed a copy of a text reflecting a posting made to Playpen from the "Broden" account, acknowledging that he had authored it.[4]

Forensic analysis of Matish's computer revealed images of child pornography, which had been deleted prior to the date of the search. Matish was later indicted on four counts of accessing with intent to view child pornography involving a prepubescent minor, based on four occasions on which he logged in to the Playpen site as the user "Broden."

[4] Matish's statements following the August 14, 2015 polygraph examination are the subject of his second motion to suppress and will be addressed more fully in the government's response to that motion.

II. The nature of Playpen and the Tor network required law enforcement to seek court approval and to deploy a NIT to identify criminals engaged in the creation, advertisement, and distribution of child pornography.

The 31-page NIT search warrant affidavit was sworn by a veteran FBI agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children. Gov't Ex. 1, p. 1, ¶ 1. It clearly and comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist in identifying registered site users who were using anonymizing technology to conceal online child sexual exploitation on a massive scale.

A. The NIT warrant set forth in great detail the technical aspects of the investigation that justified law enforcement's request to use the NIT.

In recognition of the technical and legal complexity of the investigation, the affidavit included: a three-page explanation of the offenses under investigation, Gov't Ex. 1, pp. 2-4, ¶ 4; a seven-page section setting out definitions of technical terms used in the affidavit, *id.*, pp. 4-10, ¶ 5; and a three-page explanation of the Tor network, how it works, and how users could find a hidden service such as Playpen, *id.*, pp. 10-13, ¶¶ 7-10. The affidavit spelled out the numerous affirmative steps a user would have to go through just to find the site. Indeed, the agent explained,

> Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. [Playpen] is listed in that section.

Id., pp. 12-13, ¶ 10. Thus, the agent continued, "[a]ccessing [Playpen] . . . requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." *Id.*

B. Playpen was dedicated to the advertisement and distribution of child pornography, a fact that would have been apparent to anyone who viewed the site.

The affidavit also described, in great detail and in stark terms the purpose of Playpen and why its users were appropriate targets for the NIT. Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of . . . methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes." *Id.*, p. 6, ¶ 10. More to the point, "administrators and users of [Playpen] regularly sen[t] and receive[d] illegal child pornography via the website." *Id.* The agent also explained the sheer scale of the illicit activity occurring on Playpen: site statistics as of February 3, 2015, for Playpen—which was believed to have been in existence only since August of 2014—showed that it contained 158,094 members, 9,333 message threads, and 95,148 posted messages.[5] *Id.*, p. 13, ¶ 11.

Playpen's illicit purpose was also apparent to anyone who visited it during the six months it operated before the FBI seized control of it. "[O]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." *Id.*, p. 13, ¶ 12. And the following text appeared beneath those young girls: "No

[5] As the affidavit explained, a bulletin board website such as Playpen is a website that provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Gov't Ex. 1, p. 4, ¶ 5(a).

cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." While those terms may have seemed insignificant to the untrained eye, the affiant explained, based on his training and his experience, that the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being "re-posted" to Playpen and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." *Id.*, pp. 13-14, ¶ 12. The combination of sexualized images of young girls along with these terms of art referencing image posting and large file compression unmistakably marked Playpen as just what it was—a hub for the trafficking of illicit child pornography.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site and highlighted the emphasis the registration terms placed on users avowing being identified. Users clicking on the "register an account" hyperlink on the main page were required to accept registration terms, the entire text of which was included in the affidavit. *Id.*, pp. 14-15, ¶¶ 12-13. Playpen repeatedly warned prospective users to be vigilant about their security and the potential of being identified, explicitly stating, "the forum operators do NOT want you to enter a real [e-mail] address," users "should not post information [in their profile] that can be used to identify you," "it is impossible for the staff or the owners of this forum to confirm the true identity of users," "[t]his website is not able to see your IP," and "[f]or your own security when browsing or Tor we also recomend [sic] that you turn off javascript and disable sending of the 'referer' header." *Id.*, pp. 14-15, ¶ 13. This focus on anonymity is entirely consistent with the desire on the part of Playpen administrators and users to evade detection of their illicit activities.

Once a user accepted those terms and conditions, a user was required to enter a username, password, and e-mail address. *Id.*, p. 15, ¶ 14. Upon successful registration, all of the sections,

forums, and sub-forums, along with the corresponding number of topics and posts in each, were observable. *Id.*, p. 15, ¶ 14. The vast majority of those sections and forums were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. For instance, within the site's "Chan" forum were individual sub-forums for "jailbait" or "preteen" images of boys and girls. *Id.*, p. 15, ¶ 14. There were separate forums for "jailbait videos" and "Jailbait photos" featuring boys and girls. *Id.* The "Pre-teen Videos" and "Pre-teen Photos" forums were each divided into four sub-forums by gender and content, with "hardcore" and "softcore" images/videos separately categorized for Boys and Girls. *Id.*, p. 16, ¶ 14. A "Webcams" forum was divided into Girls and Boys sub-forums. *Id.* The "Potpurri" forum contained subforums for incest and "Toddlers." *Id.*

The affidavit also described, in graphic detail, particular child pornography that was available to all registered users of Playpen, including images of prepubescent children and even toddlers, being sexually abused by adults. *Id.*, pp. 17-18, ¶ 18. Although the affidavit clearly stated that "the entirety of [Playpen was] dedicated to child pornography," it also specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id.* pp. 20-21, ¶ 27.

The affidavit further explained that Playpen contained a private messaging feature that allowed users to send messages directly to one another. The affidavit specified that "numerous" site posts referenced private messages related to child pornography and exploitation, including an example where one user wrote to another, "I can help if you are a teen boy and want to fuck your little sister, write me a private message." *Id.*, pp. 18-19, ¶ 21. According to the affiant's training and experience and law enforcement's review of the site, the affiant stated his belief that the site's private message function was being used to "communicate regarding the dissemination of child

pornography." *Id.*, p. 19, ¶ 22. The affidavit also noted that Playpen included multiple other features intended to facilitate the sharing of child pornography, including an image host, a file host, and a chat service. *Id.*, pp. 19-20, ¶¶ 23-25. All of those features allowed site users to upload, disseminate, and access child pornography. And the affidavit included detailed examples and graphic descriptions of prepubescent child pornography disseminated by site users through each one of those features. *Id.*

C. The affidavit and attachments explained what the NIT would do and precisely identified the seven pieces of information it would collect and send back to government-controlled computers.

The affidavit contained a detailed and specific explanation of the NIT, its necessity, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime.

Specifically, the affidavit noted that without the use of the NIT "the identities of the administrators and users of [Playpen] would remain unknown" because any IP address logs of user activity on Playpen would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." Gov't Ex. 1, p. 22, ¶ 29. Further, because of the "unique nature of the Tor network and the method by which the network . . . route[s] communications through multiple other computers, . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed." The affiant thus concluded, "using a NIT may help FBI agents locate the administrators and users" of Playpen. *Id.*, pp. 23-24, ¶¶ 31-32. Indeed, he explained, based upon his training and experience and that of other officers and forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence

necessary to prove . . . the actual location and identity" of Playpen users who were "engaging in the federal offenses enumerated" in the warrant. *Id.*, p. 23, ¶ 31.

In terms of the deployment of the NIT, the affidavit explained that the NIT consisted of additional computer instructions that would be downloaded to a user's computer along with the other content of Playpen that would be downloaded through normal operation of the site. Gov't Ex. 1, p. 24, ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. *Id.* The discrete pieces of information to be collected were detailed in the warrant and accompanying Attachment A, along with technical explanations of the terms. They were limited to the following: (1) the actual IP address assigned to the user's computer; (2) a unique identifier to distinguish the data from that collected from other computers; (3) the operating system running on the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's Host Name; (6) the computer's active operating system username; and (7) the computer's Media Access Control (MAC) address. *Id.*, pp. 24-25, ¶ 34.

The affidavit explained exactly why the information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." *Id.*, p. 26, ¶ 35. For instance:

> the actual IP address of a computer that accesses [Playpen] can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

Id.

The affidavit specifically requested authority to deploy the NIT each time any user logged into Playpen with a username and a password. *Id.*, p. 26, ¶ 36. However, the affidavit disclosed to the magistrate that, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation," the FBI might "deploy the NIT more discretely against particular users, including those who "attained a higher status" on the site or "in particular areas of [Playpen]" such as the sub-forums with the most egregious activity which were described elsewhere in the affidavit. *Id.*, pp. 24-25, ¶ 32, n. 8. Finally, the affidavit requested authority for the NIT to "cause an activating computer – wherever located – to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." *Id.*, pp. 29-30, ¶ 46(a).

III. Hours before the NIT warrant was signed, Playpen's administrator changed the site logo, replacing two sexually suggestive images of a prepubescent girl with one sexually suggestive image of a prepubescent girl.

As noted above, among the things described in the NIT warrant affidavit was Playpen's site logo: "on the main page of the site, located to either side of the site name, were two images depicting partially clothed prepubescent females with their legs spread apart." Gov't Ex. 1, p. 13, ¶ 12. A screenshot showing this logo as of February 3, 2015, is attached as Exhibit 3. Between September 16, 2014 and February 3, 2015, FBI agents reviewed Playpen in an undercover capacity to document the activity on the site. Gov't Ex. 1, p. 13, ¶ 11. Sometime before February 18, 2015, Playpen's administrator changed the URL—the site address. Noticing that the URL had changed, the affiant visited Playpen on February 18, 2015, and confirmed that the content had not changed. *Id.*, p. 13, ¶ 11 n.3. This includes the site logo.

In the evening of February 19, 2015, the FBI executed a search at the Florida home of the Playpen administrator and apprehended him. *Id.*, p. 23, ¶ 30. At that point, the FBI also assumed control of Playpen. Postings by the administrator from earlier in the day show that just before he was arrested, the administrator changed Playpen's site logo, replacing the images described above with a single image showing a prepubescent girl, wearing a short dress and black stockings, reclined on a chair with her legs crossed and posed in a sexually suggestive manner. A screenshot of this altered logo is attached as Exhibit 4. The text described in the affidavit as part of the logo, "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview," which the affidavit explained pertain to image distribution, remained unchanged. *Compare* Gov't Ex. 1, p.13, ¶ 12 *and* Gov't Ex. 2 *with* Gov't Ex. 3.

The NIT warrant was sworn to and authorized at 11:45 a.m. on February 20, 2015, the day after the logo change. The affidavit did not reference this change.

LEGAL STANDARD & ARGUMENT

A veteran FBI agent with nearly two decades of experience explained to a neutral and detached magistrate why there was probable cause to believe that registered users of Playpen (1) knew Playpen was a website dedicated to the sexual exploitation of children, and (2) intended to use Playpen for its express purposes—viewing and sharing child pornography. He supported this conclusion with a detailed description of the steps required to find Playpen and register as a user and the numerous indicators of Playpen's illicit purpose. That purpose was obvious to even a casual observer, but the agent also was able to bring to bear his considerable training and experience and determine that the likelihood that any user of Playpen was ignorant of the fact that it was a forum dedicated to child pornography was exceedingly low.

Relying on this information, the magistrate judge authorized the FBI to deploy a NIT to gather a limited set of identifying information from any user who logged into Playpen while it operated under FBI control. There in the warrant, plain as day, was a clear description of which computers would be searched—any computers that logged into Playpen—and seven pieces of information that would be seized. The Fourth Amendment asks no more.

As detailed below, nothing in the defendant's First Motion to Suppress undermines this conclusion. The defects he identifies, if indeed they are defects, are neither of constitutional magnitude nor the result of an intention on the part of the FBI to mislead the magistrate or skirt the rules. His contrary assertions find no support in the record. Defendants seeking the extraordinary remedy of suppression must clear a high hurdle. The defendant falls far short, and his motion should denied.

I. The NIT warrant affidavit amply supports the magistrate's finding of probable cause for issuance of the NIT warrant

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Ornelas v. United States*, 517 U.S. 690, 696 (1996). It is a fluid concept that focuses on "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (internal quotation marks omitted).

Importantly, probable cause does not require a showing of "absolute certainty," *United States v. Gary*, 528 F.3d 324, 327 (4th Cir. 2008). It demands only "a fair probability that contraband or evidence of a crime will be found in a particular place," *id.* (quoting *Gates*, 462 U.S. at 238), a finding that, in turn, "depends on the totality of the circumstances and involves a

'practical common-sense decision whether'" such a fair probability exists. *United States v. Moses*, 540 F.3d 263, 268 (4th Cir. 2008) (quoting *Gates*, 462 U.S. at 238). "This standard 'is not defined by bright lines and rigid boundaries." *United States v. Grossman*, 400 F.3d 212, 217 (4th Cir. 2005). "Instead, the standard allows a magistrate judge to review the facts and circumstances as a whole…." *Id.* (citing *United States v. Williams*, 974 F.2d 480, 481 (4th Cir. 1992)). Recognizing that reasonable minds may differ regarding whether a particular affidavit establishes probable cause, the Supreme Court "concluded that the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination." *United States v. Leon*, 468 U.S. 897, 914 (1984) (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969); *see also Grossman*, 400 F.3d at 217; *United States v. Blackwood*, 913 F.2d 139,142 (4th Cir. 1990).

"[T]he task of a reviewing court is not to conduct a *de novo* determination of probable cause, but only to determine whether there is substantial evidence in the record supporting the magistrate's decision to issue the warrant." *Massachusetts v. Upton*, 466 U.S. 727, 728 (1984). "When reviewing the probable cause supporting a warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant." *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1992) (citing *Blackwood*, 913 F.2d at 142).

A. The facts contained in the affidavit, along with the reasonable inferences to be drawn therefrom, support probable cause to believe that registered users of Playpen intended to view and trade child pornography.

The NIT warrant affidavit amply supported a finding of probable cause. The affiant, a 19-year FBI veteran with specialized training and experience in the field, set forth in detail why there was probable cause to believe anyone who logged into Playpen did so intending to view and/or trade child pornography. Accordingly, his 31-page affidavit provided ample justification

for deploying a NIT that would obtain seven discrete pieces of information and assist law enforcement in identifying those engaged in the sexual exploitation of children.

Here, the affiant's assessment—and the magistrate's reasonable reliance upon it—was supported by specific, articulable facts and inferences drawn from his training and experience. To begin, Playpen was no run-of-the-mill website that any internet user might just stumble upon. Rather, as a Tor hidden service, Playpen was accessible only to users who downloaded the necessary software and *knew* the precise algorithm-generated URL for Playpen. Gov't Ex. 1, p. 12, ¶ 10. This is so, the affiant explained, because "Tor hidden services are not indexed like websites on the traditional Internet" and so, "unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site." *Id.*

Rather, "a user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location." *Id.* Indeed, the affiant noted that there is a Tor "hidden service" page dedicated to pedophilia and child pornography that contained a section with links to Tor hidden services that contain child pornography, including Playpen. *Id.* Given this, it was no great leap in logic for the magistrate to conclude that that a user who managed to find Playpen was aware of its purpose and content.

The defendant disagrees and points to the search engine found at https://ahmia.fi as proof that the affiant's assessment about the difficulty in finding Playpen through a traditional search was incorrect. Putting to one side that his bald assertion does nothing to undermine the conclusions of a veteran FBI agent relying on his experience and that of other experts, the defendant seemingly overlooks the search engine's "[c]ontent filtering policy" that states, "[w]e

are removing each page which contains any child abuse from this search index" and provides a mechanism that users can report sites that contain child exploitation material. *See* https://ahmia.fi (last visited April 1, 2016).

Then, of course, there is the site itself, which the magistrate reasonably could have concluded would have immediately alerted any user to the fact that it contained illicit images. Upon arrival at Playpen's homepage, the affiant explained, the user saw "to either side of the site name . . ., two images depicting partially clothed prepubescent females with their legs spread apart. Gov't Ex. 1, p. 13, ¶ 12. The images alone are a strong indicator of the presence of illicit child pornography. But there was more—namely, written underneath those suggestive images of prepubescent girls were the instructions: "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview." *Id.* While perhaps not obvious to the untrained eye, the affiant explained from his training and experience, he knew that "'no cross-board reposts'" refers to a prohibition against material that is posted on other websites from being 're-posted' to the website and '.7z' refers to a preferred method of compressing large files or sets of files for distribution." *Id.* The suggestions that filenames be encrypted and that users include previews are obvious references to the sharing of image and video files. And while such references, without more, do not compel the conclusion that the images and videos being shared are necessarily illicit, that was certainly a reasonable inference to draw, particularly given the other information available to the magistrate. Magistrates are required to be neutral, not devoid of common sense, when reviewing a warrant application.

The registration terms, to which any user who wished to log into Playpen had to agree, provide further support for the inference that Playpen's users were well aware of the its illicit purpose. As detailed above, Playpen repeatedly warned prospective users about the risks of being

identified. Among other things, users were told, "the forum operators do NOT want you to enter a real [e-mail] address"; users "should not post information [in their profile] that can be used to identify [them]"; and "[t]his website is not able to see your IP." *Id.*, pp. 14-15, ¶ 13. Again, without more, these warnings may have seemed innocuous. Viewed in context, however, this focus on anonymity is entirely consistent with the desire on the part of Playpen users to avoid law enforcement detection.

Playpen's content is relevant too. As the affiant noted, upon registration, all of the sections, fora, and sub-fora were at the user's fingertips. *Id*., p. 15, ¶ 14. The vast majority were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. *Id*., pp. 15-16, ¶ 14, n.5. That none of the subsections are specifically focused on adults (other than perhaps the "Family Playpen – Incest" section) only reinforced the conclusion that users knew perfectly well Playpen's purpose. The affiant described in graphic detail particular child pornography that was available to Playpen users, pornography that depicted prepubescent children and even toddlers being sexually abused by adults. *Id*., pp. 17-18, ¶ 18. The affiant offered a litany of site sub-fora that contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id*. pp. 20-21, ¶ 27. He understandably concluded, and the magistrate reasonably found, "the entirety of [Playpen was] dedicated to child pornography." *Id.*

Courts have routinely held that membership in a child pornography website, even without specific evidence of a suspect's downloading child pornography, provides sufficient probable cause for a search warrant. This is so given the commonsense, reasonable inference that someone who has taken the affirmative steps to become a member of such a website would have accessed, received, or downloaded images from it. *See United States v. Gourde,* 400 F.3d 1065, 1070 (9th

Cir. 2006) (*en banc*) (finding sufficient probable cause for residential search where defendant paid for membership in a website that contained adult and child pornography; noting reasonable, commonsense inference that someone who paid for access for two months to a website that purveyed child pornography probably had viewed or downloaded such images onto his computer); *United States v. Martin*, 426 F.3d 68, 74-75 (2d Cir. 2005) (finding probable cause where purpose of the e-group "girls12-16" was to distribute child pornography; noting "[i]t is common sense that an individual who joins such a site would more than likely download and possess such material"); *United States v. Shields*, 458 F.3d 269 (3d Cir. 2006) (finding probable cause where defendant voluntarily registered with two e-groups devoted mainly to distributing and collecting child pornography and defendant used suggestive email address); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) ("[I]t is common sense that a person who voluntarily joins a [child pornography] group . . . , remains a member of the group for approximately a month without cancelling his subscription, and uses screen names that reflect his interest in child pornography, would download such pornography from the website and have it in his possession."); *accord United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) (suppressing evidence from residential search for lack of probable cause where defendant was never accused of actually gaining access to the website that contained child pornography, there was no evidence that the primary purpose of the website was collecting and sharing child pornography, and defendant was never said to have ever been a member or subscriber of any child pornography site).

In sum, "numerous affirmative steps" were required for a user to find and access Playpen, which made it "extremely unlikely that any user could simply stumble upon" the site "without understanding its purpose and content." Gov't Ex. 1, pp. 12-13, ¶ 10. That, combined with the information available on Playpen's homepage and registration terms, considered in light of the

affiant's specialized training and experience, even in the unlikely event that someone did stumble upon Playpen, its illicit purpose would have been obvious.

B. Matish's challenge to the magistrate's finding of probable cause utterly fails.

Nothing the defendant says in his motion casts doubt on the affiant's conclusions or the magistrate's finding of probable cause to deploy the NIT. The defendant's primary argument relies on a fundamental misunderstanding of the bases for the magistrate's finding of probable cause. Specifically, the defendant claims that, because—in his view—it is not readily apparent to a viewer of Playpen's homepage that the site is dedicated to child pornography, the NIT warrant must fail. For several reasons, his analysis misses the mark.

First, the defendant's claim that Playpen's illicit purpose was not readily apparent reflects nothing more than his disagreement with the conclusions of a seasoned FBI agent applying his considerable training and experience to the objective, observable facts. As detailed above, the sexually suggestive logo, the text that accompanied it, and the registration terms all reinforced the agent's conclusion that Playpen was no mere discussion forum or a space for users to exercise their First Amendment rights, as the defendant baldly asserts. Rather, he concluded that Playpen was obviously a forum dedicated to the sharing of child pornography and child sexual exploitation. Law enforcement officers may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person." *United States v. Johnson*, 599 F.3d 339, 343 (4th Cir. 2010) (quoting *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (collecting cases). In making probable cause determination, magistrates "may rely upon an experienced officer's conclusions as to the likelihood that evidence exists and where it is located." *United States v. Brown*, 958 F.2d 369 (4th Cir. 1992) (unpublished table decision) (collecting cases); *see*

also United States v. Terry, 911 F.2d 272, 275 (9th Cir. 1990) (quoting *United States v. Fannin*, 817 F.2d 1379, 1382 (9th Cir. 1987)); *United States v. Fauntleroy,* 800 F. Supp. 2d 676, 686 (D. Md. July 25, 2011) ("The issuing judge is entitled to rely on the affiant's training and experience on the issue whether those involved in certain types of illegality customarily store evidence in their home."). This applies with equal force in child pornography cases. *See, e.g., United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010) (finding affidavit that included statements based on affiant's training and experience regarding child pornography trafficking and storage provided substantial basis for probable cause determination); *United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000) (same). The defendant is certainly free to disagree with the affiant's assessment, but his disagreement does not mean that the magistrate was compelled to do the same.

Second, Playpen's illicit purpose was apparent was but one factor supporting the magistrate's probable cause determination. As explained in the affidavit, Playpen was no ordinary website accessible to any ordinary internet user. Access to Playpen required specialized software and knowledge of the algorithm-generated URL. The defendant raises the specter of the unwary internet traveler who might happen upon Playpen and login with every intention of engaging in legal conduct. But as the affiant explained, given the nature of Playpen and the "numerous affirmative steps" required to access it, such a scenario was exceedingly unlikely. Gov't Ex. 1, pp. 12-13, ¶ 10.

This is a critical observation because it is the exceedingly low probability that someone would happen upon Playpen ignorant of its content that shows why the lessons the defendant attempts to draw from *Gourde* and other website cases do nothing advance his cause. Def.'s First Mot. to Supp., pp. 13-16 (ECF 18). The defendant takes the government to task because the NIT warrant did nothing to distinguish between "accidental browsers" who logged into

Playpen ignorant of its illegal content and individuals seeking illegal child pornography. *Id.* at. 15-16. *Gourde*, the defendant claims, stands for the proposition that membership in a website dedicated to child pornography may support a finding of probable cause so long as this illicit purpose is readily apparent to a first-time or accidental viewer. *Id.*, p. 13-14. Even if correct, the defendant's analysis depends on there being some chance such an "accidental browser" exists, something that Playpen, by its nature and operation, makes extremely unlikely. This conclusion finds ample support in the affidavit supporting the NIT warrant, and it was entirely reasonable for the magistrate to draw that inference and authorize the warrant.

II. Matish has made no showing that justifies a Franks hearing, let alone established that the NIT warrant contained a material and intentional or reckless falsehood or omission.

"An accused is generally not entitled to challenge the veracity of a facially valid search warrant affidavit." *United States v. Allen*, 631 F.3d 164, 171 (4th Cir. 2011). "In its decision in *Franks v. Delaware*, however, the Supreme Court carved out a narrow exception to this rule, whereby an accused is entitled to an evidentiary hearing on the veracity of statements in the affidavit." *Id.* (citing *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978)). To be entitled to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978), a defendant "must make a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit." *Franks*, 438 U.S. at 155-56 (quotations omitted). When a *Franks* hearing is sought based on information omitted from an affidavit, the defendant must show: (1) that the omission is the product of a deliberate falsehood or of a reckless disregard for the truth, and (2) inclusion of the omitted information in the affidavit would defeat probable cause. *United States v. Colkley*, 899 F.2d 297, 301-02 (4th Cir. 1990); *accord Clenney*, 631 F.3d at 664-65 (affirming denial of

motion for *Franks* hearing based on omissions that were neither "designed to mislead the magistrate" nor "material"). In addition to this substantial preliminary showing, a defendant must also demonstrate that the alleged falsity or omission was material to the probable cause determination. *Franks*, 438 U.S. at 155-56; *accord United States v. McKenzie-Gude*, 671 F.3d 452, 462 (4th Cir. 2011); *United States v. Cioni*, 649 F.3d 276, 286 (4th Cir.), *cert. denied*, 132 S. Ct. 437 (2011); *United States v. Clenney*, 631 F.3d 658, 663 (4th Cir. 2011); *and Allen*, 631 F.3d at 171. For materiality, the central question is whether the inclusion in the affidavit of the "deliberately omitted facts" would "defeat the probable cause showing and thus render false the original 'literally true' affidavit." *United States v. Tate*, 524 F.3d 449, 456-57 (4th Cir. 2008). This is so because the purpose of a *Franks* hearing is "to prevent the admission of evidence obtained pursuant to warrants that were issued only because the magistrate was misled into believing that there existed probable cause." *United States v. Friedemann*, 210 F.3d 227, 229 (4th Cir.), *cert. denied*, 531 U.S. 875 (2000) (emphasis added).

In the seminal case, *Franks v. Delaware*, the Supreme Court stressed that there is a presumption of validity with respect to a search warrant affidavit. 438 U.S. at 155-56. As such, under *Franks*, conclusory allegations of a defect will not do. *Id.* at 171. Defendants must offer allegations of intentional falsehood accompanied by an offer of proof. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished or their absence satisfactorily explained before a hearing is granted. *Id.; see also United States v. Chandia*, 514 F.3d 365, 373 (4th Cir. 2008). Allegations of negligence or innocent mistake are insufficient. *Franks*, 438 U.S. at 171. In *Franks* and subsequent cases, the Supreme Court was clear that the rule it had announced has "a limited scope," one that places a heavy burden on the defendant. *Id.* at 169; *see also United States v. Jeffus*, 22 F.3d 554, 558 (4th Cir. 1994). A defendant

cannot meet that burden through a conclusory argument based on "bare allegations" that fail to make the requisite preliminary substantial showing. *United States v. Chandia*, 514 F.3d 365, 373 (4th Cir. 2008).

Applying these principles, there can be little doubt that the defendant has not made anything resembling a substantial, preliminary showing of an intentional or reckless falsehood or omission. First, his offer of proof hardly suffices. He proffers no evidence that any omission of the administrator's change to the Playpen logo just before the NIT warrant was authorized was reckless, let alone intentional. Nor could he. After all, the affiant explained that he had reviewed Playpen on February 18, 2015, the day before the logo changed. Gov't Ex. 1, pp. 14-15 n.3. The most that can be said is that, with the benefit of hindsight, it would have been better for the affiant to have reviewed Playpen the morning the warrant was signed, as opposed to two days before. If a failing at all, which is by no means obvious, it was—at worst—an unintentional oversight. Indeed, it would be a stretch to characterize the agent as negligent; it certainly cannot be said he acted recklessly or with some intent to deceive. And, "mere[ ] negligen[ce] in . . . recording the facts relevant to a probable-cause determination" is not enough to warrant a *Franks* hearing. *Colkley*, 899 F.2d at 301 (quoting *Franks*, 438 U.S. at 170). Similarly, a "good faith mistake" by the affiant will not invalidate the warrant. *See id.*

Just as important, even if that omission were intentional, it was utterly immaterial to the finding of probable cause. The administrator's replacing *two* sexually suggestive images of prepubescent girls with *one* sexually suggestive image of a prepubescent girl is hardly the game changer that the defendant claims it to be. The defendant derives significance from the fact that, in his view, the logo and the two images that were present until the day before the NIT warrant was authorized form the *sine qua non* of the probable cause finding. That the defendant say it is so,

however, does not make it correct. As detailed above, the magistrate's probable cause finding rested on a host of facts and inferences resting on the affiant's specialized training and experience that demonstrated a "fair probability" that anyone who logged into Playpen did so intending to view and/or share child pornography. The relevance of the image(s) in the Playpen logo was that it/they sexualized young girls. That was true before February 19, *see* Gov't Ex. 2, and it remained true after, *see* Gov't Ex. 3.

Nor do the other purported misstatements the defendant identifies warrant a *Franks* hearing. Indeed, much of what he characterizes as "false statements" reflect little more than his opinion about the weight the Court should attach to particular statements in the affidavit and the affiant's training and experience. For example, the defendant takes issue with the affiant's claim that Playpen was "dedicated to child pornography"; disputes the significance of the affiant's description of the text contained underneath those suggestive images on the website's main page; and disagrees with the affiant's assessment that accessing Playpen required "numerous affirmative steps" that made it "extremely unlikely that any user could simple stumble upon" the site "without understanding its purpose and content." *See* Def.'s First Mot. to Supp. at 9-10, 12, 16-17 (ECF 18). The defendant's mere disagreement with the affiant's description of the facts or the inferences to be drawn from those facts in light of his training and experience, however, does not an omission or falsehood make.

The defendant is certainly free to contest whether the facts contained in the affidavit, considering the totality of the circumstances, supported probable cause—as he apparently does. He is not, however, entitled to a *Franks* hearing simply because he does not like the inferences drawn from those facts by the affiant. And he certainly cannot convert his disagreement into a showing that the affidavit was somehow misleading just by declaring it so. Nothing in *Franks*

requires an affiant to "list every conceivable conclusion" and his failure to do so in no way "taint[s] the validity of the affidavit." *Colkley*, 899 F.2d at 301 (quoting *United States v. Burnes,* 816 F.2d 1354, 1358 (9th Cir.1987)) (internal quotation marks omitted).

Even so, beyond conclusory assertions that a particular statement is wrong or "nonsense," the defendant offers nothing that would suggest it constitutes an intentional or reckless falsehood. "*Franks* clearly requires defendants to allege more than 'intentional' omission in this weak sense." *Colkley*, 899 F.2d at 301. "To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Franks*, 438 U.S. at 171. The defendant's remaining "*Franks*" arguments are exactly that: reflective of little more than his apparent desire to cross-examine the affiant.

The defendant also makes much of the fact that Playpen provided a chat forum for its members. He maintains that the affiant's characterization of Playpen as a site dedicated to child pornography swept too broadly, preventing the magistrate from considering the "substantial First Amendment rights" that were implicated. Def.'s First Mot. To Supp. at 21 (ECF 18). It seems odd for the defendant to describe this as an omission given that the affiant did not omit the chat feature provided by Playpen. Gov't Ex. 1, pp. 19-20, ¶¶ 23-25. In any event and more importantly, the affiant also noted that even this chat feature served Playpen's illicit purpose. *Id.* In particular, the affiant provided specific examples of Playpen's chat feature being used for the purpose of distributing child pornography. *Id.*, p. 20, ¶ 25.

In short, the sum total of the defendant's *Franks* argument seems little more than a recitation of his principal argument against the finding of probable cause: that is, it was theoretically possible that a user may have accessed Playpen without intent to view child pornography. The affiant did not claim otherwise. He merely concluded, based upon the

available facts and his training and experience, that it was "extremely unlikely." Gov't Ex. 1, pp. 12-13, ¶ 10. More importantly, the magistrate agreed.

III. The NIT warrant particularly described the locations to be searched and the things to be seized based on a showing of probable cause as to each.

The NIT warrant described the places to be searched—activating computers of users or administrators that logged into Playpen—and the things to be seized—the seven pieces of information obtained from those activating computers—with particularity. And a neutral and detached judge found that there was probable cause to support the requested search. The Fourth Amendment requires no more. Accordingly, the Court should decline the defendant's invitation to read into the Fourth Amendment a heretofore undiscovered upper bound on the number of searches permitted by a showing of probable cause.

The constitutional principles at play here are well settled. "[N]o warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Constitution demands that two things be described with particularity: "'the place to be searched' and 'the persons or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006). As to the place, it must be described with sufficient particularity "such that the officer with a search warrant can, with reasonable effort, ascertain and identify the place intended." *United States v. Owens*, 848 F.2d 462, 463 (4th Cir. 1988) (quoting *Steele v. United States*, 267 U.S. 498, 503 (1925)) (internal quotation marks omitted). As to the items seized, nothing must be "left to the discretion of the officer executing the warrant" in deciding what to seize. *Marron v. United States*, 275 U.S. 192, 196 (1927). Whether this particularity standard is met is determined in light of the information available at the time the warrant issued. *Owens*, 848 F.2d at 463-64.

The Fourth Amendment also places limits on the scope of a search. "When a search is conducted pursuant to a warrant, it 'is limited in scope by the terms of the warrant's authorization.'" *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *United States v. Phillips*, 588 F.3d 218, 223 (4th Cir.2009)). "[T]he scope of a lawful search 'is defined by the object of the search and the places in which there is probable cause to believe that it may be found.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (quoting *United States v. Ross*, 456 U.S. 798, 824 (1982)). Under this principle, "[a] lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search." *United States v. Ross*, 456 U.S. 798, 820-21 (plurality opinion). Thus, for purposes of the Fourth Amendment, determining the proper scope of a search depends on the relationship between the items to be seized under the warrant and the likelihood that they will be found in the places to be searched.

Plainly, the NIT warrant meets both particularity requirements. Attachments A and B of the NIT warrant were, respectively, identified the "Place to be Searched" and the "Information to be Seized." Both defined with precision where agents could look and for what. The warrant authorized deployment of the NIT to the computer server hosting Playpen and then to computers of "any user or administrator who logs into [Playpen] by entering a username and password." Gov't Ex. 1, Att. A. Attachment B, in turn, imposed precise limits on what information could be obtained from those computers by the NIT:

1) the computer's actual IP address and the date and time that the NIT determines what that IP address is;

2) a unique identifier generated by the NIT to distinguish data from that of other computers;

3) the type of operating system running on the computer;

4) information about whether the NIT has already been delivered to the "activating" computer;

5) the computer's Host Name;

6) the computer's active operating system username; and

7) the computer's media access control ("MAC") address.

Id., Att. B.

Tellingly, the defendant does not claim that the locations to be searched were not readily identifiable from the face of the warrant or that the warrant somehow left the decision of what should be seized open to debate. Nor does he claim that there is any doubt that the items authorized to be seized were not reasonably likely to be found in the places to be searched. Rather, he presses a novel constitutional rule for the Internet age: the NIT warrant is an unconstitutional "general warrant" because it authorized, upon finding of probable cause, the collection of specific information from a potentially large number of computers. If he is right, then hidden within the Fourth Amendment is a previously undiscovered upper bound on the number of search locations a showing of probable cause can support.

To be sure, the Fourth Amendment demands that there be probable cause to search a particular location for particular items. But the notion that a warrant supported by sufficient probable cause to authorize a search of numerous locations is, for that reason alone, constitutionally defective is absurd. Either probable causes *exists* to support a search or searches or it *does not*. Here, of course, the defendant maintains that the NIT warrant, which permitted the collection of information from any user or administrator who logged into Playpen, was not supported by sufficient facts to justify the search. As explained above, however, he is incorrect. There was a *fair probability* that anyone who logged into Playpen did so with knowledge of its

content and the intent to consume it. Accordingly, the warrant properly authorized the deployment of the NIT to any such user, regardless of how many there are or could be.

Curiously, the defendant finds support for his argument in the affiant's disclosure to the magistrate that, although it sought authority to deploy the NIT to any user who logged into Playpen, the FBI might deploy the NIT in a more targeted fashion—*e.g.*, those users who accessed parts of Playpen containing the most egregious examples of child pornography. Gov't Ex. 1, p. 24, n.8. The defendant's point seems to be that because the FBI could execute the warrant more narrowly, it is constitutionally compelled to do so. The Fourth Amendment's particularity requirement countenances no such rule, however. A warrant is "facially deficient" only when it fails to provide any meaningful instruction to the searching agents regarding the items to be seized. *See Marron*, 275 U.S. at 196; *United States v. Ruhe*, 113 F.3d 1233 (4th Cir. 1997) ("A warrant that fails to particularize the place to be searched or the items to be seized is so facially deficient that it precludes reasonable reliance only when '[o]fficers poised to conduct a search [would] be able to ascertain that [it] fails to offer sufficiently detailed instruction and instead leaves them guessing as to their task.'" (quoting *United States v. Towne*, 997 F.2d 537, 549 (9th Cir.1993) (alterations in original)) (unpublished table decision). That the FBI retained discretion to execute the warrant on a narrower set of users does not somehow convert it into an unconstitutional general warrant.

Nor do the defendant's entreaties for the Court to look to the Ninth Circuit's decisions concerning electronic searches get him anywhere. Def.'s First Mot. to Supp. at 25 (ECF 18). He is certainly correct in noting that the Ninth Circuit has cautioned its magistrates to be vigilant in approving electronic searches to strike "the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."

United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc). But, the NIT warrant hardly can be described as the sort of "general exploratory" search over which that Circuit has expressed concern. The defendant's effort to cast the NIT warrant as authorizing a sweeping electronic search of personal data strains credulity. The limited scope of the NIT warrant's authorized search is certainly relevant in assessing its reasonableness and the magistrate's determination. The NIT warrant did not subject the defendant to a wholesale search of his electronic devices. Rather, the NIT collected seven pieces of information that would assist law enforcement in identifying those suspected of trading and viewing child pornography.

Indeed, the most critical piece of information obtained by the NIT warrant—the defendant's IP address—is information that ordinarily would have been publicly available over which the defendant cannot claim a reasonable expectation of privacy. *In re Application of the U.S. for an Oder Pursuant to 18 U.S.C. § 2703*, 830 F. Supp. 2d 114, 131 (E.D. Va. 2011) (concluding that "IP addresses . . . are a fundamental part of the Internet's architecture, and cannot be eliminated from Internet communication without rendering the technology useless;" while it "can be masked or obfuscated by using intermediary computers . . . the IP address information itself is a functional necessity" and, as such, the communication to a third-party website of that information "by using Internet-connected devices to access . . . accounts, demonstrate[ed] voluntary assent to whatever disclosures would be necessary to complete the communications"); *In re § 2703(d)*, 787 F. Supp. 2d 430, 438-440 (E.D. Va. Mar. 11, 2011) (holding that petitioners "have no Fourth Amendment privacy interest in their IP addresses" because, "like a phone number, an IP address is a unique identifier assigned through a service provider" that "corresponds to an internet user's individual computer," one that can be "voluntarily conveyed . . . thus exposing the information to a third party administrator, and thereby relinquishing any reasonable

expectation of privacy" (internal citations omitted)); *see also United States v. Suing*, 72 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers"); *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [Internet Service Providers]."); *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007) (Internet users have no expectation of privacy in the IP addresses of the websites they visit). Importantly, those courts who have considered the question have expressly concluded that the use of the Tor network does not change the result. *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 28, 2016) (concluding that a Playpen user "has no reasonable expectation of privacy in the most significant information gathered by deployment of the NIT, [his] assigned IP address," because even though "the IP addresses of users utilizing the Tor network may not be known to websites, like [Playpen], using the Tor network does not strip users of all anonymity, because users accessing [Playpen] must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific location"); *United States v. Farrell*, No. CR15-029RAJ, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016) (considering the question as applied to the administrator of a site on the Tor network through which illicit substances were distributed and concluding that users of the network "must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations," and that "[u]nder th[o]se circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network"); *see also* 811 F.3d 275, 278 (8th Cir. 2016) ("An Internet Service Provider (ISP) assigns an IP address to an individual

computer using its Internet service and associates the IP address with the physical address to which that service is being provided.").

In short, the defendant's novel rule, which he cloaks in the language of particularity and overbreadth as if to conceal its lack of constitutional foundation, cannot defeat a validly obtained warrant, supported by probable cause, that particularly describes where to search and for what. That a warrant authorizes the search of a potentially large number of suspects is an indication, not of constitutional infirmity, but a large number of criminal suspects.

IV. Matish's remaining claim that the warrant is void because the "triggering event" never occurred also fails.

The defendant's claim that the NIT warrant was void because, as an anticipatory warrant, the "triggering event" never occurred is little more than a rehash of the same probable cause and *Franks* challenges that have already been addressed. Although the defendant does not appear to challenge the notion that the NIT warrant could be categorized as an anticipatory warrant, he wrongly asserts that it was void because the "triggering event" that would authorize its execution against him never occurred. Def.'s First Mot. to Supp. at 26-28 (ECF 18).

It is well settled that the Fourth Amendment is no bar to "anticipatory warrants." These warrants are "no different in principle from ordinary warrants." *United States v. Grubbs*, 547 U.S. 90, 96-97 (2006).

> [T]wo prerequisites of probability must be satisfied. It must be true not only that if the triggering condition occurs "there is a fair probability that contraband or evidence of a crime will be found in a particular place," but also that there is probable cause to believe that the triggering condition will occur.

Id. (quoting *Gates*, 462 U.S. at 238).

Here, the relevant "triggering event" was the defendant's decision to enter his username and password into Playpen and enter the site. (Although, as was the case with many other users,

the NIT was not deployed to the defendant immediately upon login but once he accessed a particular section of the site.) And here, too, the NIT warrant affidavit provided ample support for the probable cause determination as to both. Attachments A and B, which were incorporated into the warrant, specified the exact conditions under which the NIT was authorized to be deployed—*i.e.*, when a user such as the defendant logged into Playpen—and as discussed in detail above, there was probable cause to believe that any user who logged on to Playpen was seeking child pornography.

The defendant posits that because the "triggering event" never occurred because the defendant did not log in to Playpen through the login page, as it was described in the NIT warrant affidavit, based on the change to the Playpen logo. Because the login page reflected this single change, the defendant asserts that the NIT warrant was void. Notably, he is not claiming that he did not, in fact, log into Playpen. Instead, the defendant's argument on this point is just a recitation of his probable cause and *Franks* challenges. As noted above, there was ample support for the magistrate's finding of probable cause, and the defendant utterly fails in his effort to make out a *Franks* challenge to the warrant. Accordingly, his claim about the absence of a "triggering event" to support execution of the NIT warrant must also fail.

V. None of Matish's claimed defects in the NIT warrant justify the extraordinary remedy of suppression and, even if that warrant does not satisfy the Fourth Amendment, the good faith exception bars suppression.

As a threshold matter, the defendant's dissatisfaction with having been discovered through the NIT is understandable. But the mere fact that he objects to having been unmasked, without more, does not warrant suppression of evidence obtained pursuant to a warrant issued by a neutral and detached magistrate based on a finding of probable cause. For all of the reasons outlined above, the NIT warrant does not contravene the requirements of the Fourth Amendment. But

even if it did, suppression of the information derived from the execution of that warrant is not appropriate.

The Fourth Amendment's exclusionary rule does not provide "a personal constitutional right, nor is it designed to redress the injury occasioned by an unconstitutional search." *Davis v. United States*, 131 S. Cr 2419, 2426-27 (2011) (quoting *Stone v. Powell*, 428 U.S. 465, 468 (1976)) (internal quotation marks omitted). The exclusionary "rule's sole purpose … is to deter future Fourth Amendment violations." *Davis*, 131 S. Ct. at 2426 (collecting cases). The real deterrent value "is a 'necessary condition for exclusion,' but it is not a 'sufficient' one." *Id.* at 2427 (quoting *Hudson v. Michigan*, 547 U.S. 586, 596 (2006)). There are substantial costs associated with its application. *Id.* ("Exclusion exacts a heavy toll on both the judicial system and society at large…. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence."). The practical effect in nearly every case "is to suppress the truth and set the criminal loose in the community without punishment." *Id.* (citing *Herring v. United States*, 555 U.S. 135, 141 (2009)). Accordingly, it is to be employed "only as a 'last resort'"—that is, when "the deterrence benefits of suppression … outweigh its heavy costs." *Id.* (quoting *Hudson*, 547 U.S. at 591); *United States v. Stephens*, 764 F.3d 327, 335 (4th Cir. 2014) ("[E]xclusion of evidence has 'always been [the] last resort, not [the] first impulse.'" (quoting *Hudson*, 547 U.S. at 591) (alterations in original)). "Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield meaningful deterrence, and culpable enough to be worth the price paid by the justice system." *Id.* (quoting *Davis*, 131 S. Ct. at 2427).

Under the good faith exception to the Fourth Amendment's exclusionary rule, suppression is not warranted when officers rely in good faith on an objectively reasonable search warrant

issued by a neutral and detached judge. *United States v. Leon*, 468 U.S. 897, 900 (1984). This objective standard is measured by "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at 922 n.23. "[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Id.* at 922 (internal quotation marks omitted). The Supreme Court observed that "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Id.* at 918. The Court identified only four circumstances in which exclusion of evidence seized pursuant to a warrant is appropriate. Those are when: (1) the issuing magistrate was misled by the inclusion of knowing or recklessly false information; (2) the issuing magistrate wholly abandoned the detached and neutral judicial role; (3) the warrant is facially deficient as to its description of the place to be searched or the things to be seized; or (4) the affidavit upon which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely on it in good faith. *Id.* at 923-924. None apply here.

Here, the NIT warrant affidavit contained no knowingly or recklessly false information that was material to the issue of probable cause. Nor does the defendant allege that the issuing magistrate abandoned her judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. And the affidavit made a strong, comprehensive showing of probable cause to deploy the NIT. Absent any of these errors, once the magistrate signed the warrant, having been made aware of how the NIT would be implemented and its reach, the agents' reliance on that authority was objectively reasonable. *See Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984) ("[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the

warrant he possesses authorizes him to conduct the search he has requested."). Ultimately, agents acted reasonably in relying on the magistrate's authorization of the NIT warrant, and so the evidence seized pursuant to it should not be suppressed.

CONCLUSION

For the foregoing reasons, the defendant's First Motion to Suppress the information identifying his home computer recovered pursuant to a search warrant that authorized the use of the network investigative technique should be denied.

Respectfully submitted,

DANA J. BOENTE
UNITED STATES ATTORNEY

By: _____/s/_____
Kaitlin C. Gratton
Assistant United States Attorney
Virginia State Bar Nos. 83935
Fountain Plaza Three, Suite 300
721 Lakefront Commons
Newport News, VA 23606
Phone: (757) 591-4000
Fax: (757)591-0866
Email: kaitlin.gratton@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 4th day of April, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Andrew W. Grindrod
Assistant Federal Public Defender
Office of the Federal Public Defender
150 Bousch Street, Suite 403
Norfolk, Virginia 23510
Andrew_Grindrod@fd.org

_____/s/_____
Kaitlin C. Gratton
Virginia State Bar No. 83935
Assistant United States Attorney
Attorneys for the United States
United States Attorney's Office
Fountain Plaza Three, Suite 300
721 Lakefront Commons
Newport, VA 23606
Phone: 757-591-4000
Email: kaitlin.gratton@usdoj.gov